



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Peter Szor

Assignee: Symantec Corporation

Title: KERNEL MODE OVERFLOW ATTACK PREVENTION SYSTEM AND

METHOD

Unknown

Serial No.: 10/781,207 Filed: February 17, 2004

2182

Group Art Unit:

Docket No.: SYMC1048

Examiner:

Monterey, CA May 25, 2004

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant(s) wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner.

U.S. PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	NAME
1)	5,696,822	12/09/97	Nachenberg
2)	5,822,517	10/13/98	Dotan
3)	6,301,699	10/09/01	Hollander et al.
4)	6,357,008	03/12/02	Nachenberg

OTHER DOCUMENTS

1)	Szor, P., U.S. Patent Application Serial No. 10/360,341, filed February 6, 2003, entitled "SHELL CODE BLOCKING SYSTEM AND METHOD".
2)	Szor, P., U.S. Patent Application Serial No. 10/371,945, filed February 21, 2003, entitled "SAFE MEMORY SCANNING".

GUNNISON, McKAY & HODGSON, L.L.P. 1900 Garden Road Montercy, CA 93940 (831) 655-0880 Fax (831) 655-0888

Serial No. 10/781,207

3)	Szor, P., U.S. Patent Application Serial No. 10/464,091, filed June 17, 2003, entitled "SEND BLOCKING SYSTEM AND METHOD".
4)	Szor, P., U.S. Patent Application Serial No. 10/611,472, filed June 30, 2003, entitled "SIGNATURE EXTRACTION SYSTEM AND METHOD".
5)	Szor, P., U.S. Patent Application Serial No. 10/681,623, filed October 7, 2003, entitled "UNMAPPED CODE BLOCKING SYSTEM AND METHOD".
6)	Szor, P., "Attacks on WIN32", Virus Bulletin Conference, October 1998, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 57-84.
7)	Szor, P., "Memory Scanning Under Windows NT", Virus Bulletin Conference, September 1999, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-22.
8)	Szor, P., "Attacks on WIN32-Part II", Virus Bulletin Conference, September 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 47-68.
9)	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
10)	Buysse, J., "Virtual Memory: Windows NT® Implementation", pp. 1-15 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://people.msoe.edu/~barnicks/courses/cs384/papers19992000/buyssej-Term.pdf.
11)	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:www.windowslibrary.com/Content/356/06/2.html.
12)	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/kernekmode.asp. No author provided.
13)	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/interception.asp. No author provided.
14)	Kath, R., "The Virtual-Memory Manager in Windows NT", pp. 1-11 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/dngenlib/html/msdn_ntvmm.asp?frame=true.
15)	Szor, P. and Kaspersky, E., "The Evolution of 32-Bit Windows Viruses", Windows & .NET Magazine, pp. 1-4 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.winnetmag.com/Articles/Print.cfm?ArticleID=8773.
16)	Szor, P., "The New 32-bit Medusa", Virus Bulletin, December 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 8-10.

17)	Szor, P., <i>"Shelling Out"</i> , Virus Bulletin, February 1997, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 6-7.
18)	McCorkendale, B. and Szor, P., "Code Red Buffer Overflow", Virus Bulleting, September 2001, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 4-5.
19)	Nachenberg, C., "A New Technique for Detecting Polymorphic Computer Viruses", University of California, Los Angeles, 1995.
20)	"INFO: CreateFileMapping() SEC_* Flags", pp.1-2 [online]. Retrieved on September 24, 2003. Retrieved from the internet: URL:http://support.microsoft.com/default.aspx?scid=http://support. microsoft.com:80/support/kb/articles/Q108/2/31.asp&NoWebContent=1. No author provided.
21)	"CreateFileMapping", pp. 1-5 [online]. Retrieved on September 10, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/fileio/base/createfile mapping.asp?frame=true. No author provided.

A PTO form 1449 listing these documents is enclosed.

Citation of the above documents shall not be construed as:

- 1. an admission that the documents are necessarily prior art with respect to the instant invention;
- 2. a representation that a search has been made, other than as described above; or
- 3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

The Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 25, 2004.

Attorney for Applicant(s)

May 25, 2004
Date of Signature

Respectfully submitted,

Serge J. Hodgson

Attorney for Applicant(s)

Reg. No. 40,017

(831) 655-0880

								ļ	Sheet	1 of 7	
Form PTO	-1449				Atty Docke	t No.		Seria	l No.		
E					SYMC1048 10/781,207						
(8 E 30)	MERRI	MATION DISCLOSU	RE CITATION	ī	Applicant(s)						
700		IN AN APPLICA	rion		Peter Sz	or					
ust ?	XX XX		Filing Date	e		Group	-				
A	Ûse	several sheets if	necessary)		February	17, 2004		2182			
WENT &	IN AN APPLICATION Peter Szor Filing Date February 17, 2004 U.S. PATENT DOCUMENTS Applicant(s) Peter Szor Filing Date Group 2182										
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS		LING D	ATE PRIATE	
	AA	5,696,822	12/09/97	Nachenberg		380	4				
	AB	5,822,517	10/13/98	Dotan		395	186				
	AC	6,301,699	10/09/01	Hollander et al.		717	4				
	AD	6,357,008	03/12/02	Nachenb	erg	713	200				
	AE										
	AF				· <u>-</u> .				·		
	AG										
	AH				<u></u>					-	
	AI										
	AJ										
	AK										
			FOREIG	N PATENT	DOCUMENTS	• S					
								2	rans	lation	
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLASS	S YES	3	мо	

								Translation		
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO		
	AL									
	AM									
	AN									
	AO									
-	AP									

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

•	AR				Application CODE BLOCKIN			10/360,341, JD METHOD".	filed	February	6,
	AS				Application EMORY SCANNI		No.	10/371,945,	filed	February	21,
	AT	Szor,	P., U.S.	Patent .	Application	Serial	No.	10/464,091,	filed	June 17,	

2003, entitled "SEND BLOCKING SYSTEM AND METHOD".

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO	Form PTO-1449					et No.	Serial No.				
					SYMC1048 10/781,207						
]	INFOR	MATION DISCLOS	URE CITATIO	N	Applicant	(s)					
		IN AN APPLIC	ATION		Peter Szor						
					Filing Dat	te		Group			
	(Use	e several sheets i	f necessary)		February	7 17, 2004		2182			
	-		v. s	. PATENT I	OCUMENTS						
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS	9 1	FILING DATE IF APPROPRIATE		
	AA								-		
	AB										
	AC										
	AD										
	ΑE										
	AF								_		
	AG										
	AH		-		· ··· - ·						
	AI										
	AJ										
	AK	120									
		· · · · · ·	FOREI	GN PATENT	DOCUMENT	'S	I				
								Tran	slation		
·		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	мо		
	AL										
	AM										
	AN	 - ···									
	AO										
	AP								1		
	<u> </u>	OTHER DOCUME	NTS (Includi	ng Author, '	Title, Date,	. Pertinent B	Pages, Etc				
-	AR	Szor, P., U.S 2003, entitle						led June	30,		
	AS	Szor, P., U.S 2003, entitle	. Patent Ap d "UNMAPPED	plication CODE BLO	Serial N CKING SYS	o. 10/681, TEM AND ME	623, fi THOD".	led Octob	per 7,		
	AT	Szor, P., "At Bulletin Ltd,	tacks on WI. The Pentag	N32", Viron, Abing	us Bullet don, Oxfo	in Confere rdshire, E	nce, Oc Ingland,	tober 199 pp. 57-8	98, Virus 34.		
Examiner			Date Consi	dered							
EXAMINER: through ci to applica	tation	al if reference con if not in conform	onsidered, whe	ther or not considered.	citation is Include co	s in conforma	nce with form with	MPEP 609; next commu	draw line nication		

Form PTO	orm PTO-1449					et No.	Serial No.			
					SYMC1048	3		10/781,	207	
] 1	NFOR	MATION DISCLOS	URE CITATIO	N	Applicant	(s)	-			
		IN AN APPLIC	ATION		Peter Sz	zor				
					Filing Date Group					
	(Use	several sheets i	f necessary)		February	7 17, 2004		2182		
			U.S	. PATENT I	OCUMENTS					
EXAMINER	·	DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS			
INITIAL								IF APP	ROPRIATE	
	AA									
	AB	1								
	AC									
	AD			<u> </u>						
•	ΑE									
	AF									
	AG									
	AH									
	AI									
	AJ						 			
	AK									
	AIX	<u> </u>	PODET	CM DAMENM	DOCUMENT	<u> </u>	<u> </u>			
			FOREI	GN PATENT	DOCUMENT			Tra	nslation	
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS		NO NO	
		DOCUMENT NOMBER	DATE	COONTRI		CHASS	SUBCLIAS	5 165	NO	
	AL									
	AM						<u> </u>			
	AN									
	AO									
	AP				_					
		OTHER DOCUME	NTS (Includi	ng Author, '	Title, Date,	. Pertinent F	Pages, Etc	2.)		
•	AR	Szor, P., "M September 19 England, pp.	99, Virus Bu	<i>ing Under</i> ulletin Lt	Windows lad, The Pe	<i>NT"</i> , Virus entagon, A	Bullet: bingdon	in Confe	rence, shire,	
-	AS	Szor, P., "A 2000, Virus I 47-68.	t <i>tacks on W</i> Bulletin Lto	<i>IN32-Part</i> d, The Per	II", Viruntagon, Al	us Bulleti pingdon, O	n Confe xfordsh	rence, Se ire, Engl	eptember land, pp.	
	AT	Chien, E. and Buffer-Overf September 20 England, pp.	l <i>ow Techniq</i> 02, Virus Bu	ues In Cor	mputer Vi:	ruses", Vi	rus Bull	letin Con	nference,	
Examiner			Date Consi	dered						
EXAMINER: through cit to applica	tation	al if reference c if not in confor								

Form PTO	-1449				Atty Dock	et No.		Serial No.	-	
					SYMC1048	3		10/781,2	07	
1	NFOR	MATION DISCLOS	URE CITATIO	N	Applicant	(s)				
		IN AN APPLIC	ATION		Peter Szor					
					Filing Dat	te		Group		
	(Use	several sheets i	f necessary)		February	7 17, 2004		2182		
			v.s	. PATENT	DOCUMENTS					
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	CLASS SUBCLASS FILI			
	AA									
	AB									
	AC									
	AD									
	AE									
	AF									
	AG									
	AH									
	AI									
-	AJ									
	AK									
			FOREI	GN PATENT	DOCUMENT	'S				
								Trans	slation	
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	мо	
	AL									
	AM									
	AN									
	AO									
	AP									
		OTHER DOCUME	NTS (Includi	ng Author,	Title, Date,	, Pertinent E	ages, Etc	.)		
	AR	Buysse, J., [online]. Ret URL:http://pe	rieved on A	April 16,	2003. Ref	trīeved fr	om the	internet:	ıyssej-	
	AS	Dabak, P., Bo pp. 1-8 [onl: URL:http://ww	ine]. Retrie	eved on Ar	oril 16; 2	2003. Retr	ieved fr	System Ser	rvices", nternet:	
	АТ	"How Entercept Retrieved on URL:http://www.provided.	April 16, 2	2003. Reti	rieved fro	om the int	ernet:			
Examiner			Date Consi	dered					···	
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).										

Form PTO	-1449)			Atty Docke	et No.		Serial No.					
					SYMC1048 10/781,207								
I	NFOR	MATION DISCLOS	URE CITATIO	N	Applicant(s)								
		IN AN APPLIC	ATION		Peter Szor								
					Filing Dat	:e		Group					
	(Use	e several sheets i	f necessary)		February	17, 2004		2182					
			บ. ร	. PATENT 1	DOCUMENTS								
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLASS	FILING I					
	AA			-									
	AB												
	AC												
	AD		-						-				
	AE												
	AF												
•	AG												
:	AH												
	ΑI												
	АJ												
	AK												
			FOREI	GN PATENT	DOCUMENT	'S	·	<u> </u>					
-								Trans	lation				
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLASS	YES	NO				
	AL												
	AM												
	AN								1				
	AO	-											
	AP												
		OTHER DOCUME	NTS (Includi	ng Author,	Title, Date,	Pertinent P	Pages, Etc	.)	<u> </u>				
	AR	"How Entercep Retrieved Apr URL:http://ww provided.	il 16, 2003	. Retriev	ed from t	he interne	t:		o author				
	AS	Kath, R., "Th Retrieved on URL:http://ms asp?frame=tru	April 16, 2 dn.microsof	003. Retr	ieved fro	m the inte	rnet:						
	АТ	Szor, P. and Windows & .NE Retrieved fro URL:http://ww	T Magazine, m the inter	pp. 1-4 net:	[online].	Retrieved	on Apr	il 16, 20					
Examiner			Date Consi	dered									
through ci	tation	n if not in confor	EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).										

Form PTO	orm PTO-1449					et No.	Serial No.				
					SYMC1048	3		10/781,2	207		
]]	NFORM	MATION DISCLOS	URE CITATIO	N	Applicant(s)						
		IN AN APPLIC	ATION		Peter Szor						
					Filing Date Group						
	(Use	several sheets i	f necessary)		February	7 17, 2004		2182			
			v.s	. PATENT I	DOCUMENTS						
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS		DATE COPRIATE		
	AA			· ·							
	AB										
	AC										
	AD										
•	AE										
	AF										
	AG										
	AH										
	AI										
	AJ										
	AK										
			FOREI	GN PATENT	DOCUMENT	:s					
								Tran	slation		
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	NO		
	AL										
	AM										
	AN										
	AO						, ,				
•	AP										
`		OTHER DOCUM	ENTS (Includi	ng Author,	Title, Date,	, Pertinent E	Pages, Etc	.)	· ·		
•	AR	Szor, P., "T Bulletin Ltd									
	AS	Szor, P., "S. Ltd, The Pen							etin		
	AT	McCorkendale September 20 England, pp.	01, Virus B								
Examiner			Date Consi	dered							
EXAMINER: through ci to applica	tation	al if reference c if not in confor	onsidered, whe	ther or not considered.	citation is Include co	s in conforma	nce with form with	MPEP 609; onext commun	draw line		

Form PTO-1449					Atty Docket No.			Serial No.		
					SYMC1048 1			10/781,2	10/781,207	
INFORMATION DISCLOSURE CITATION					Applicant(s)					
		IN AN APPLIC	Peter Szor							
					Filing Date Group					
(Use several sheets if necessary)					February 17, 2004			2182		
U.S. PATENT DOCUMENTS										
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS	FILING DATE IF APPROPRIATE		
	AA				-					
	AB									
	AC									
	AD									
	AE									
,	AF						i.		· · ·	
•	AG									
	AH									
	AI				**				· ·	
	AJ									
	AK									
FOREIGN PATENT DOCUMENTS										
								Tran	slation	
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	мо	
	AL									
-	AM									
}	AN								-	
	AO									
4	AP							_		
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)										
•	AR Nachenberg, C., "A New Technique for Detecting Polymorphic Computer Viruses", University of California, Los Angeles, 1995.									
	AS	"INFO: CreateFileMapping() SEC_* Flags", pp.1-2 [online]. Retrieved on September 24, 2003. Retrieved from the internet: URL:http://support.microsoft.com/default.aspx?scid=http://support.microsoft. com:80/support/kb/articles/Q108/2/31.asp&NoWebContent=1. No author provided.								
	АТ	"CreateFileMapping", pp. 1-5 [online]. Retrieved on September 10, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/fileio/base/createfilemapping. asp?frame=true. No author provided.								
Examiner Date Co			Date Consid	sidered						
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).										